DOE F 1325.8

ed States Government | Department of Energy

Albuquerque Operations Office

memorandum

DATE: May 3, 2000

REPLY TO: ICSD:LPL

SUBJECT: Inspection Plan for LANL Survey

TO: Richard F. Lucero, Acting Chief, IPB, SPSD

Attached, are documents that I will use for the Operations Security functional area of the LANL survey. If you have questions in this regard, I may be reached at 845-5242.

Lowell Preston Little, OCP, CPP
Operations Security Manager
Intelligence and Cyber Security Division

Attachments

Reviewed 5/4/00

VII. OPERATIONS SECURITY

Description

OBJECTIVE. The OPSEC Program is a process designed to disrupt or defeat the ability of foreign intelligence or other adversaries to exploit sensitive Departmental activities or information and to prevent the unauthorized disclosure of such information.

INDICATORS OF EFFECTIVENESS: Indicators of the effectiveness of an OPSEC program may be found in certain key elements, such as:

- Are as many people as possible involved? An effective program must rely on the regular input of many people.
- Are there steady levels of activity? While occasional focused efforts are necessary (e.g., an OPSEC Assessment of a new program), a sound program requires a continuous level of distributed activity.
- Does the OPEC program have a high degree of visibility? An effective OPSEC program thrives on visibility; be visible to everyone at a facility, from top to bottom.
- Does the OPSEC program have credibility? Representing OPSEC in ways that fit in with the organization's culture will inspire confidence and invoke trust in the program.
- Is the technology understood? Effective OPSEC managers understand the technical side of the organizations' functions, and can communicate about technical requirements with a real understanding of their impact on facility operations.
- Is the focus on achievement? Is proactive rather than reactive change emphasized? Effective program management has a vision of what they want to accomplish and focus on achieving it.
- Is there a "big-picture" perspective? In addition to handling day-to-day problems, effective OPSEC managers must take time to consider both internal and external events and their likely impact on operations security.
- Is there an open and honest path of information: Sharing information with others is important in resolving situations.
- Are there effective countermeasures in place to frustrate the intelligence cycle? Do the countermeasures complement other security measures?
- Is OPSEC discussed at Security Education briefings? If so, does the OPSEC program manager provide the information?
- Does the OPSEC Program apply the five-step process, i.e., Identify Critical Information, Analyze Threat, Analyze Vulnerabilities, Assess Risk, and Apply Countermeasures?
- Does the OPSEC program manager conduct and review results of self-assessments?

OTHER CONSIDERATIONS: Special attention should be give to address concerns such as Industrial Espionage, Intellectual Properties, Technology Transfer, CRADA, and Treaty Related Concerns. Consideration must be given to special access requirements, such as Sensitive Compartmented Information and Special Access Programs, as they relate to the OPSEC program.

References:

Survey Content

Evaluation of the implementation and management of the OPSEC Program, to include administration, procedures, scheduling, reporting, tracking of services and corrective actions, and other elements essential to a viable OPSEC program. Key program elements to be reviewed include the OPSEC Manager, OPSEC Working Groups, OPSEC Program Plan, and OPSEC Program Files.

Documentation

DOE O 471.2 requires the development and maintenance of certain documentation. Specific OPSEC program documentation to be developed and maintained are:

- OPSEC Plan
- OPSEC Procedures
- OPSEC Program Files
- Local Threat Statement
- Critical and Sensitive Information List
- Essential Elements of Friendly Information
- Counter-Imagery Program Plan (if applicable)

Interviews

- OPSEC Program Manager
- CI Program Manager
- OPSEC Working Group Chairperson
- Director/Manager of Safeguards and Security
- Classification Officer
- Contracting Officer
- Program/Project Manager of selected sensitive activities.

DOE Albuquerque Operations Office
Safeguards and Physical Security Division
Security Programs and Site Support Branch

Material Control and Accountability Program Survey Plan

Los Alamos National Laboratory

Los Alamos, New Mexico
September 10-15, 2000

Approved By:

Cindy Murdock

Cindy Murdock
Survey MC&A Topic Team Lead
Revision 1.0

Facility Name, Location, Station:

Los Alamos National Laboratory
Los Alamos, New Mexico
AUA

Survey Dates:
September 10-15, 2000

Facility Description:

The Los Alamos National Laboratory (LANL) is a government owned facility operated by the University of California under the auspices of the DOE Albuquerque Operations Office. The primary mission of the Laboratory is to develop world class science and technology and apply them to the Nation's security and well being. The Laboratory provides technical assistance to the DOE complex, supports DOE's research mission and completes work for other federal agencies, including the nation's defense and intelligence agencies. The LANL mission requires the handling and storage of Category I quantities of special nuclear material (SNM) and other nuclear materials. LANL is a Category I facility.

Survey Scope:

The survey will include document reviews, records reviews, interviews, observations, and performance testing. These survey techniques will be used to conduct compliance and performance reviews of the following Material Control and Accountability (MC&A) program elements: Program Administration, Administrative Controls, Nuclear Material Inventories, Nuclear Material Measurements, Nuclear Material Accounting, and Nuclear Material Control. These six program elements are combined and rated as three topics: Basic Requirements, Material Accountability, and Material Control. Because these three rating topics are not equal, they will be given the following weighting relative to one another when determining the overall rating of the MC&A program: Basic Requirements (Program Administration, Administrative Controls – 2), Material Accountability (NM Inventories, Accounting, Measurements – 3), and Material Control (1). The DOE O 474.1 and DOE M 474.1-1 will be the basis for conducting the reviews, with special emphasis on prior survey findings, corrective actions, and performance.

Survey Team Members:

Cindy Murdock, Physical Scientist, NNSA/AL
John M. Andrews, General Engineer, NNSA/AL
S. Andrew Sandoval, Auditor, NNSA/AL
Usha I. Narayanan, Physical Scientist, DOE/CH, New Brunswick Laboratory
Sherri Cross, MC&A Team Lead, DOE/RFFO
Albert G. Garrett, Security Specialist, DOE/RFFO

LANL 2000 Safeguards and Security Survey
MC&A Team
Schedule of Activities

Sunday, September 10, 2000		
Time	*Activity*	*Participants*
10:00 am – 5:00 pm	Survey Team Meeting Data Call Document Review Location: TA-35 Meeting Area	AL Survey Team

Monday, September 11, 2000		
Time	*Activity*	*Participants*
7:30 am	MC&A Team Planning	MC&A Survey Team
9:00 am	Joint Safeguards and Security In-Brief Location: Los Alamos Area Office, Room 100	AL/LAAO/LANL Management LANL POCs Survey Team
1:00 pm	MC&A In-Brief Document Requests Scheduling	MC&A Team
4:00 pm	MC&A Team Meeting LAAO MC&A Office	MC&A Team
5:00 pm	Survey Team Meeting, TA-54	Survey Team

Tuesday, September 12, 2000		
Time	*Activity*	*Participants*
AM	MASS Accounting System Review	Sandoval
	Accounting Procedures Waste Accounting	Sandoval
	Measurement Methods Precision and Accuracy Goals and Values Not Amenable to Measurement	Narayanan
	Defense in depth Insider Analysis Rollup Studies Separation of Duties	Andrews, Murdock, Garrett, Cross
PM	Batch Accounting and Reconciliation Process	Sandoval, Murdock, Andrews

Tuesday, September 12, 2000		
Time	*Activity*	*Participants*
	Measurement Methods Precision and Accuracy Goals and Values Not Amenable to Measurement	Narayanan
	Defense in depth Insider Analysis Rollup Studies Separation of Duties	Garrett, Cross
4:00 pm	MC&A Team Meeting LAAO MC&A Office	MC&A Team
5:00 pm	Survey Team Meeting TA-54	Survey Team

Wednesday, September 13, 2000		
Time	*Activity*	*Participants*
AM	CMR Facility Tour Materials and Activities Wing 9 Vaults Material Control Elements Portal Monitoring Daily Administrative Controls	Murdock, Garrett, Cross
	Eternal Transfers DOE Form 741 Reviews	Sandoval
	NDA Measurement Review	Narayanan
	IRA Program Plans and Procedures Schedule of Assessments Reports – timeliness Resolution of IRA findings/concerns – tracking Performance Testing	Andrews
PM	Material Control Procedures	Garrett, Cross
	MC&A Program – independence from line organizations, authorities and responsibilities	Murdock, Andrews
	Mass and Bulk Measurement Review	Narayanan

Wednesday, September 13, 2000		
Time	*Activity*	*Participants*
	TID Program Review	Sandoval
4:00 pm	MC&A Team Meeting LAAO MC&A Office	MC&A Team
5:00 pm	Survey Team Meeting TA-54	Survey Team

Thursday, September 14, 2000		
Time	*Activity*	*Participants*
AM	TA-55 Facility Tour Materials and Processes Vaults Material Control Elements Portal Monitoring Daily Administrative Controls	Garrett, Cross, Murdock
	Chemistry Measurement Review	Narayanan
	Internal Transfers NMMSS Reconciliation	Sandoval
	Finding Resolution and Closure	Andrews
PM	TA-18 Facility Tour Materials and Activities Vaults Material Control Elements Portal Monitoring Daily Administrative Controls	Garrett, Cross, Murdock, Narayanan
	TA-18 Internal Transaction/MASS Access Controls	Sandoval
	Occurrence Investigation and Reporting	Andrews
4:00 pm	MC&A Team Meeting LAAO MC&A Office	MC&A Team
5:00 pm	Survey Team Meeting TA-54	Survey Team

Friday, September 15, 2000		
Time	*Activity*	*Participants*
AM	Followup Finalization of Any Findings	MC&A Team
12:00	Data Gathering Ends No findings issued after this Point	Survey Team
2:00 earlier ↑	Survey Team Murder Board All Topical Ratings have to be Assigned and Rationale Documented	Survey Team
3:00	Working Close Out All Findings Presented included References And Requirements (No Impact)	Survey Team AL Management LAAO Management LANL Management

Survey Plans for Each MC&A Topical Area

D.1. Basic Requirements

D.1.1 Program Administration

1. Review all Program Planning Documentation to ensure that it is complete and covers the entire MC&A program.
2. Validate that LANL has obtained all required DOE/AL approvals.
3. Review the MC&A Plan to ensure that it is complete and addresses all applicable DOE requirements.
4. Review deviations from DOE order requirements to validate that LANL has obtained all required DOE approvals.
5. Review MC&A procedural directives to ensure that they are documented and have appropriate approvals.
6. Review the site's SSSP.
7. Review emergency plan, including facility specific emergency evacuation procedures.

D.1.2 Administrative Controls

1. Review the internal review and assessment program to ensure that it addresses all elements of the MC&A program.
2. Validate that the facility has a performance testing program that tests all critical elements of the MC&A program.
3. Review occurrence investigation and reporting program to ensure that it is functional and effective.
4. Review finding resolution and closure for the MC&A program to ensure that findings are tracked and closed appropriately.
5. Review access controls to nuclear material data and data generating equipment.

D.2 Material Accountability

D.2.1 Nuclear Material Inventories

1. Review the program used to implement graded safeguards to ensure that all accountable quantities of nuclear materials are entered into the accounting records and protected at the appropriate levels.
2. Review the programs for source and other nuclear materials to determine how they are being accounted for and protected (graded safeguards).
3. Review the programs for terminating or reducing safeguards to ensure that the proper program approvals are documented and that radiological sabotage threats are being evaluated before termination of safeguards.
4. Review physical inventory practices and procedures to ensure that the inventories provide material is present in its purported quantity and location.
5. Review the basis for physical inventory sampling plans to ensure that they are statistically valid.

D.2.2 Accounting

1. Review the accounting structure to ensure that it localizes inventory differences at the MBA level.
2. Review the accounting system and records to ensure that they document all nuclear material transactions in accordance with the DOE requirements and generally acceptable accounting principles.
3. Review the nuclear material transactions to ensure that they properly document the activity and movement of material.
4. Review the NMMSS reporting to ensure that all external transactions and internal adjustments are properly reported and documented.

D.2.3. Measurements

1. Review the Measurement Program to ensure that the measurement systems used to perform safeguards measurements provide accurate nuclear material accountability values.
2. Review the Measurement Program organization(s) to ensure it is independent and those involved in the program are knowledgeable.
3. Review the Measurement Program to ensure that measurement controls are developed and implemented for all measurement systems used to perform safeguards measurements.

D.3. Material Control

1. Review the TID program to ensure completeness.
2. Review the program for monitoring and evaluating material control indicators, i.e., inventory differences (IDs), shipper/receiver differences (SRDs), and normal operating losses (NOLs).
3. Review the program for authorizing, documenting, tracking, and verifying material transfers.
4. Review waste monitoring practices to ensure that all waste streams are being monitored out of TA-55, the CMR, and TA-18.
5. Review SNM Portal Detection program to verify compliance with DOE order requirements.
6. Review the elements of the MC&A program that ensure nuclear materials are being used, processed, and stored within the appropriate boundaries.
7. Review the material surveillance program to ensure that it can detect unauthorized activities or anomalous conditions and report on material status.
8. Review the material access program to ensure that it controls access to nuclear materials according to DOE 5632.1C-1.

LANL 2000 Safeguards and Security Survey

Inspection Plan – Program Planning

Documentation

- LANL budget documents
- LANL staffing documents
- SSSP defining future resources
- Documentation addressing new S&S requirements
- Docuentation of LANL upgrades e.g. PIDAS and complementary S&S upgrades

Interviews

- LANL S&S Program Manager responsible for development of S&S budget
- LANL S&S Program Managers responsible for providing input to staffing levels
- LANL S&S Director responsible for approving budget and staffing levels
- PTLA Manager responsible for requesting dollars and staffing level for the protective force

Performance Measures

Upon completion of the review of documentation and interviews and daily meeting with the other team members to get feedback regarding any lack of resources, the inspectors will be able to analyze and determine the degree of effectiveness of LANL's program planning. The documentation will be used to evaluate projected needs for funding, staffing, and upgrades to ensure an effective S&S program. The reviews conducted by the balance of the survey team will be used to determine any deficiencies in staffing/personnel and any significant programmatic deficiences that have not been addressed. In addition, the interviews will identify any constraints which would not allow LANL to obtain desired/projected resources. Other forms of measurement may also be developed to assist the survey team in determining the effective of LANL's S&S program planning.

Questions for Program Planning

Goal 1 – Does LANL S&S have plans/procedures designed to implement, manage and maintain the S&S Programs?

1. Does LANL S&S have organizational goals/objectives? At what organizational level? Do they have set of actions required?

2. Who approves goals/objectives?

3. Does LANL have a plan/procedure for reaching goals? Include documented assumptions? Do they have a schedule? Are S&S staff aware of the goals?

4. Does LANL have a system for determining needs for improvement? (self-assessment, PAP, survey findings, OA inspection findings, etc)

5. Are resources committed to reach the goals/objectives? Who approves resources for both dollars and personnel?

6. Do the members of the organization carry on activities consistent with the chosen goals/objectives?

7. Is progress toward the goals/objectives monitored and measured to assure performance conforms to the plans? (Pert chart or Gantt chart used)

8. Does LANL take corrective action if progress is unsatisfactory?

Goal 2 – How are forecasts used in support of or planning for the S&S program. (new technology, intelligence information, new DOE Orders, new policy {in memo form} and new programs)?

1. Are technology changes considered in LANL protection strategy? (palm pilots, pagers, explosive detection, weapons, etc.)

2. How does LANL use intelligence information in planning?

3. How does LANL address implementation of new requirements such as a new DOE Order or policy memorandum?

4. Does S&S get involved in new programs at LANL? At what point in the process?

Goal 3 – Does LANL have plans to sustain the site protection program during planned improvements/upgrades/revisions?

1. Does LANL have a plan for maintaining site S&S during construction of new PIDAS?

2. Does LANL have a plan for cut over of the new Argus Alarm Monitoring System?

Goal 4 – Does LANL plan for contingencies?

1. Has LANL changed any contingency planning as a result of the recent fire?

2. Does LANL have a contingency plan for guard force strikes, complete failure of the alarm monitoring system, etc.?

Goal 5 – Does LANL have any current or projected operational constraints that affect planning?

1. Does S&S have limits placed on the dollar amount placed in the budget(s)?

2. Are there any staffing constraints placed on S&S?

3. Does the operating organizations place any constraints on S&S that affect planning?

Evaluate

VIII. SURVEYS AND SELF-ASSESSMENTS

The Survey and Self-Assessment Programs encompass on-site examinations of the safeguards and security measures implemented for the protection of DOE S&S facilities, activities, and interests. S&S suveys and self-assessments provide assessments of adequacy and effectiveness, survey team will inspect this subtopic to determine if survey and self-assessment programs are conducted for all approved facilities/subcontractors.

POLICY AND GUIDANCE

Includes the applicable chapters in DOE O 470.1A, Chapters IX and X, and the AL policy memorandum dated December 11, 1997, subject: Guidance on the Conduct of Self-Assessments.

- SURVEYS

Purpose: Ensure that surveys have been conducted on all applicable facilities. Facilities that are eligible to have access to, use, store, or transmit nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat and/or classified information, that require access authorizations, or that possess over $5,000,000 of DOE property, exclusive of facilities and land values.

Possessing facilities under LANL's cognizance include (all "A" facilities):

Facility Code 123, Los Alamos National Laboratory
Facility Code 6037, Los Alamos National Laboratory (SCIF at Los Alamos)
Facility Code 341, Los Alamos National Laboratory (Nevada Test Site Operations) (inspected by NV).

LANL is not the designated responsible office for any "B," "C," "PPA," or "D" facility clearances.

LANL is the designated responsible office for 104 "NP" facility clearances. The Defense Security Service is the Cognizant Security Agency for 22 of these facility clearances and as such, has inspection responsibility. The Albuquerque Operations Office is responsible for the inspections of the other 82, which includes two excluded parent facility clearances.

- SELF-ASSESSMENTS **(Deemed a Special Emphasis area for this survey)**

Purpose: Self-assessments are to be used as a management tool to determine S&S program status and to identify areas needing special attention.

Procedures: Formal procedures, e.g., operating instructions, in place to address all areas.

Self-Assessment Plan: A general plan is required.

Special Emphasis Areas: Areas should be identified and reviewed based upon new requirements, changes to security areas, results of other inspections, etc. Must be included in plan.

Frequency of Self-assessments. Shall be ongoing, performed on an annual basis and scheduled "between" periodic surveys, not included extensions.

Areas (subtopics) identified as being deficient as a result of trend analyses conducted of security-related incidents.

Documentation of Self-Assessment

- Documents
  - LANL Self Assessment Procedures
  - AL " Policy

- CORRECTIVE ACTIONS in regard the both surveys and self-assessment will be covered under "Resolution of Findings."

Documentation

- Survey and Self-Assessment Program Plans
- Implementing Procedures
- Survey and Self-Assessment Reports
- Corrective Action Plans
- Validation and Closing Procedures
- Process for determining inspectors' qualifications (and possibly the documentation showing the qualifications.)

Interviews

- Management responsible for S&S survey and self-assessment programs
- Management responsible for S&S-related survey and self-assessment activities
- S&S Program Managers
- Self-assessment inspectors
- Individual(s) responsible for deficiency resolution.

Performance Measures

After the completion of document reviews, interviews, and observation of the day-to-day activities, the team will be able to measure how effectively the S&S survey and self-assessment programs have been implemented. Other forms of measurement may also be developed to assist the survey team in determining the effectiveness of the programs.

Goal 1 Determine compliance to A) LANL SA procedure and B) AL policy

Goal 2 Determine that people conducting the SA have the necessary expertise.

97 & 99 by DP? Goal 3 Determine that SA was comprehensive

Focus on 2000

Approach: Meet initially with program mgr for SA
Divide up and meet with people who conducted subtopics SA assess expertise comprehensiveness
Have all inspectors evaluate SA on com... their subtopic for feedback

recovery plan from fire?
on-schedule?
... of Emphasis determined

Resolution of Findings

LANL Survey Plan
September 11-15, 2000

Description: Self-Assessments, surveys, and inspections may result in the identification of discrepancies or findings in the Safeguards and Security program at a facility. The management must ensure that the findings from these reviews are documented properly, monitored, and resolved in a timely fashion.

Purpose of the Survey: To determine the degree and extent of management involvement in the resolution of findings process and how well LANL has implemented policy, resolved findings and issues, documented findings, met milestones, and developed corrective actions to ensure discrepancies do not reoccur.

Survey Conduct: The survey will be conducted through data collection and documentation reviews, observations, and interviews.

References:

- DOE O 470.1, Safeguards and Security Program, 9/28/95.

Survey Content:

Evaluation and validation of survey reports, self-assessment reports, corrective action plans, implementing procedures, validation and closing procedures, and documented budget for S&S will provide the current status, management support, and direction for correcting identified S&S program deficiencies.

Interviews will be conducted with the Division Director, Program Manager responsible for Resolution of Findings, subject matter experts, and individuals responsible for implementation of action plans.

Observation of the day-to-day processes will be undertaken to determine the completeness and effectiveness of the program.

Incident Reporting and Management

LANL Survey Plan

~~May 8-19~~, 2000

SEPT. 11-15

Description: Incidents of safeguards and security concern are events that, at the time of occurrence, have yet to be determined a violation of law, but that are of such concern to the safeguards and security program as to warrant immediate review, inquiry, and subsequent assessment and reporting. The LANL Incident Reporting and Management Program is responsible for deterring, detecting, and ensuring the prompt reporting of incidents of security concern to DOE. This includes the systematic conduct of inquiries into the circumstances surrounding an incident, the development of pertinent information, and the determination of an infraction, criminal violation, or loss.

Purpose of the Survey: To determine how well LANL has implemented policy on incidents of safeguards and security concerns.

Survey Conduct: The survey will be conducted through data collection and documentation reviews, observations, and interviews.

References:

- DOE O 2030.4B, Reporting Fraud, Waste, and Abuse to the Office of Inspector General, 5/18/92.
- DOE O 232.1A, Occurrence Reporting and Processing of Operations Information, 7/21/97.
- DOE M 232.1, Manual for Occurrence Reporting and Processing of Operations Information, 9/25/95.
- DOE O 470.1, Safeguards and Security Program, 9/28/95.
- DOE O 471.2A, Information Security Program, 3/27/97.
- DOE G 471.2-1, Classified Matter Protection and Control Implementation Guide, 11/95.
- DOE M 471.2-1B, Classified Matter Protection and Control Manual, 1/6/99.
- Memo, Kirkman/Distribution List, Subject: Policy for Reporting Incidents of Security Concern, 11/26/99.
- Memo, Mahaley/Distribution List, Subject: Implementation for Reporting Security Incidents to the Office of Security Affairs, 10/18/99.
- Memo, Glauthier/Various, Subject: Reporting Security Incidents, 9/7/99.
- Memo, Gioconda/Operations Office Managers, Subject: Security Incident and Infraction Reporting, 8/8/99.

Survey Content:

Evaluation of initial notification and status reports, occurrence reporting and incident reporting procedures, post orders, inquiries, and corrective action tracking documentation to determine their effectiveness and whether procedures were followed for incidents that occurred since 1999 survey. Oral reporting procedures regarding ORPS incidents will also be evaluated for consistency and immediacy. Performance will be measured by determination that incident reports (including pro force reports, inquiry reports, status reports, and infraction forms) and ORPS are detailed and accurate, reporting timelines were met, and integration of incident and ORPS reporting with other S&S procedures is effective.

Interviews will be conducted with the Contractor Program Managers responsible for S&S Incident and ORPS Programs (including computer security), Contractor Inquiry Officials, Protective Force Manager, and a random selection of employees to determine the consistency and effectiveness of the S&S incident program.

INDIVIDUAL INSPECTION PLANS

Los Alamos National Laboratory

Safeguards and Security survey

July 23 – August 9, 2001

Los Alamos National Laboratory
Periodic Safeguards and Security Survey
July 23 through August 3, 2001
Inspection Plan - PROTECTION PROGRAM OPERATIONS

I. INTRODUCTION

This topical area covers DOE activities directed toward the protection of DOE property from adversary actions that would have an adverse impact on the national security, the health and safety of employees, the public or the environment. These activities, or programs, include physical security; security systems; protective force operations; security badges, shields and credentials; and transportation security. The goal of this program is to prevent malevolent acts that may include: theft, diversion, industrial sabotage, radiological sabotage, destruction, riots, terrorism, espionage, unauthorized access, loss or compromise, or other hostile acts. The "Design Basis Threat Policy for the Department of Energy Programs and Facilities" (U), and vulnerability assessments will be used in conjunction with local threat guidance for the development and implementation of the Protection Program Operations program. This program should be documented and described in great detail in the facility's Site Safeguards and Security Plan (SSSP).

The Protection Program Operations program should include a strategy for protecting each safeguards and security interest. Protection strategies include the denial, containment, recapture/recovery and pursuit. Denial and containment strategies rely upon physical security, security systems, and PF personnel. The type of strategy used will be determined by the impact that a malevolent act would have on national security, the health and safety of DOE and DOE contractor employees, the environment, the public, or loss or damage of Government property.

Protection Program Operations should provide a graded level of protection that accomplishes the safeguards and security mission in an efficient and cost-effective manner. Ideally, there should be a complete overlap of the performance of the protection system and compliance with DOE orders.

References

The compliance segment of a facility survey reflects the status of the facility's safeguards and security system as measured against implementation of applicable Federal statutes, regulations, policy, and approved safeguards and security plans. Each inspector is responsible for reviewing the appropriate statues, regulations, policy and plan. The following is a list of DOE references that apply to this section:

- 10 CFR, Part 710, "Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Significant Quantities of Special Nuclear Material"

- Title 10 CFR 1046, "Medical and Physical Fitness Standards for Protective Force Personnel"
- Title 10 CFR 1047, "Limited Arrest Authority and Use of Force by Protective Force Personnel"
- Title 42 U. S. C. 2011, et seq., "Atomic Energy Act of 1954"
- DOE Order 5480.16a, "Firearms Safety"
- DOE Order 5632.1c, "Protection and Control of Safeguards and Security Interests"
- DOE Manual 5632.1c-1, "Manual for Protection and Control of Safeguards and Security Interests"
- DOE Order 5632.7a, " Protective Force Program"
- DOE Manual, "Firearms Qualification Courses Supplement," August 1997
- DOE Order 6430.1a, "General Design Criteria"
- DOE Order 470.1, "Safeguards and Security Program"
- DOE Order 471.1, "Identification and Protection of Unclassified Controlled Nuclear Information"
- DOE Order 471.2a, "Information Security Program"
- DOE Manual 471.2-1b, "Classified Matter Protection and Control Manual"
- DOE Notice 473.1, "Carrying Semiautomatic Pistols with a Round in the Chamber"
- DOE Manual 473.2-1, "Firearms Qualification Courses Manual"
- DOE Notice 473.2, "Standardization of Firearms"
- DOE Notice 473.4, "Department of Energy Badges"
- DOE Notice 473.5, "Security Area Vouching and Piggybacking"
- DOE Order 474.1, "Control and Accountability of Nuclear Materials"
- DOE Manual 474.1-1, "Manual for Control and Accountability of Nuclear Materials"
- DOE Manual 475.1-1, "Identifying Classified Information"
- "DOE Security Container and Locking Device Guide," December 1993

References should also include the Los Alamos National Laboratory SSSP, Protective Force orders and response plans, alarm maintenance procedures, and other applicable documents.

Survey Content

Evaluation of the Protection Program Operations includes a review of management support/involvement, administration of the program elements, funding and staffing to implement the protection programs, planning (safeguards and security as well as safety), reporting, and other activities associated with the Protection Program Operations program.

Documentation

The SSSP and local operating procedures will be reviewed. Additionally, there will be contingency/emergency plans and plans for the support by outside federal and local law enforcement agencies. From these documents, the survey team will become familiar with the site layout, site mission, and identify potential targets as part of the survey planning process. Additional documentation may be requested while conducting the on-site survey activities.

Interviews

Meetings will be scheduled and Interviews conducted with laboratory management personnel responsible for the implementation of the Protection Program Operations to include:

- Safeguards and Security Division Director and/or Deputy Director
- Office of Security Inquiries Acting Office Leader
- Site Safeguards and Security Planning Team Leader
- Program Integration Group Leader
- Security Systems Group Leader
- Physical Security Team Leader
- Badge Office Team Leader
- Human Reliability Team Leader
- Protective Force General Manager
- Protective Force Training Manager
- Protective Force Operations Manager
- Protective Force Budget Director
- Protective Force Field Operations Division Commander
- Protective Force Special Operations Division Commander
- Protective Force Line Supervisors

Subtopical Areas

The following subtopical areas comprise Protection Program Operations:

A. Physical Security
B. Security Systems
C. Protective Force
D. Security Badges, Credentials, and Shields
E. Transportation Security

A. Physical Security

Physical Security comprises the physical protection of security interests to include Special Nuclear Material (SNM) and Vital Equipment, Sensitive Information, Departmental Property and Unclassified Facilities. An effective Physical Security Program will have taken the following items into consideration when developing their protection program strategy:

- The vulnerability of SNM, vital equipment or facilities, or sensitive matter to malevolent acts
- The importance of the facility to the overall DOE mission and costs of replacement
- The classification level of the matter and the impact of its loss or compromise on national security

- The potential effects of a malevolent act on the health and safety of employees, the environment, or the public
- The need for compartmentalization of safeguards and security interest
- The need for efficient and cost-effective methods for protecting the safeguards and security interests based upon DOE order requirements and performance based tests

Survey Content

Evaluation of the planning, implementation, and management of the Physical Security Program should include planning documents, management support/involvement, administration of the program, staffing qualifications, reporting, and other activities associated with the Physical Security Program. The main elements to be surveyed are:

- Protective Lighting
- Physical Barriers
- Fences
- Walls, Ceilings, and Floors
- Doors
- Windows
- Unattended Openings
- Vehicle Barriers
- Security Containers
- Personnel and Vehicle Access Control
- Property Protection

Documentation

The following documents must be available for review before the survey begins and during the remainder of the survey process:

- SSSP (if no SSSP, then SSP(s))
- Lock and Key records and procedures
- Property control and removal procedures
- Access control procedures
- Local performance testing plans, procedures, test results, corrective actions, and other records
- Identification of security areas and safeguards and security interests

All documentation must be in compliance with DOE Orders, and should identify inconsistencies and contradictions. The documentation should provide the inspector a thorough understanding of the protection programs of the facility and should assist in the development of system performance testing if required. Finally, the documentation should point to any deviations to DOE Orders.

Interviews

Interviews will be conducted to ensure that those responsible for this program are knowledgeable of DOE requirements, site procedures, and technical requirements. Interviews will be conducted with the Team Leader responsible for physical security as well as with members of his/her staff.

Performance Measures

The goal of the physical security survey is to ensure that the protective systems and subsystems perform as intended and designed. To accomplish this goal, inspectors will conduct basic performance tests. Performance tests may be announced or unannounced. Unannounced performance tests will be coordinated with the laboratory's Point of Contact for the subtopical area. Performance tests must be performed in a manner to minimize operational impact while promoting optimal safety.

B. Security Systems

The ultimate objective of a physical security systems is protecting SNM, vital equipment, classified information, DOE property, and unclassified facilities is determined by examination and testing of construction, facilities, and equipment. A physical security system consists of buildings, fences, barriers, lighting, sensors, surveillance devices, entry control devices, access control systems, protective personnel posts, central alarm station/secondary alarm stations (CAS/SAS), power systems, and other real property and hardware designed for or affecting security. The essential elements of these security systems are detection, assessment, delay, and response. Security plans and security equipment should enhance and contribute to an effective response to an adversarial act.

An effective security systems program will be tailored to address specific site characteristics and requirements, current technology, ongoing programs, operational needs, and acceptable protection levels that reduce inherent risks on a cost-effective basis. Intrusion Detection Systems (IDS) are to be installed at applicable security boundaries to provide reasonable assurance that breaches of security boundaries are detected and that timely detection of unauthorized access attempts and information is provided to protective force personnel. IDS will ensure all safeguards and security targets are provided protection for early detection and provide an effective way to assess all non-scheduled alarms whether they are real, false, nuisance, or tamper.

Survey Conduct

The main elements to be inspected are the design, installation, maintenance, and testing procedures and practices. Inspectors will test the alarm systems (or review test records) to determine if the alarm systems provide real time annunciation sufficient to ensure adequate time for the security force to respond effectively. Inspectors will determine if the barriers deny penetration or provide sufficient information and intelligence about the adversary to allow

the Protective Force to interdict adversary actions effectively. Inspectors will also review the primary and alternate communications equipment to determine if they are functional and of a design that allows for the Protective Force to respond effectively. Finally, inspectors will review compensatory measures and determine if they are adequate to compensate for any system deficiencies.

CAS/SAS operators will be interviewed to determine their understanding of how the system operates and their responses to alarm conditions. In addition, inspectors must review CAS/SAS operators' qualifications to ensure they have received adequate training and have been qualified to perform in their assignments.

The process of evaluation includes assessing the results of document reviews, interviews, and performance tests. Key elements for this evaluations are:

- Intrusion Detection Systems
- Close Circuit Television (CCTV) systems (Assessment Capabilities)
- Communication networks to include line supervision
- CAS/SAS
- False Alarm Rates (FAR) and Nuisance Alarm Rates (NAR)
- Power Supplies
- Contingency Plans and Procedures
- Portal Monitors
- Sensitivity requirements
- Calibration and Maintenance
- Life Cycle Management

Documentation

The following documentation will be reviewed:

- SSSP
- Physical Security System description(s) and location(s)
- Maintenance and testing records and procedures
- Unscheduled Alarm Reports
- Calibration procedures and records
- CAS/SAS procedures
- Emergency response for CAS/SAS recovery
- Emergency power systems
- Compensatory procedures for equipment outages

Interviews

Inspectors will conduct interviews with the following:

- Safeguards and security staff responsible for Security Systems
- SPOs and SOs
- Engineers (responsible for the Security System(s))
- Alarms maintenance/installation and testing personnel
- CAS/SAS Management
- CAS/SAS Operators
- Protective Force Managers
- Other personnel responsible for walk testing systems

Performance Measures

The goal of performance tests is to confirm the ability of operating system elements or total systems to meet established protection requirements. A well-developed maintenance and testing program will demonstrate that the systems operate according to DOE standards. Security systems selected for evaluation will be performance tested by walking through the paths they are designed to protect. Tamper alarms will be tested as well. Lighting and back-up power will be tested to ensure compliance with DOE standards. CCTV systems will be evaluated to determine adequacy and ability to meet established goals for assessment.

C. PROTECTIVE FORCE

The PF protects DOE safeguards and security interests from theft, diversion, industrial sabotage, radiological sabotage, toxicological sabotage, espionage, unauthorized access, loss or compromise, and other hostile acts that may cause unacceptable adverse impacts on national security, program continuity, the environment, or the health and safety of employees and the public.

Protective personnel who are armed protect life and property at DOE facilities as authorized by 10 CFR 1047.

To fulfill this mission, the PF must have proper management and supervision, a comprehensive, well-documented formal training program, and sufficient quantities of appropriate, well-maintained, and properly deployed equipment and facilities. Protective personnel must possess both routine and tactical skills to enable them to perform their mission as individuals or as a team.

Survey Content

Evaluation of the planning, implementation, and management of the PF will include development and implementation of planning documents, management support/involvement, administration of the program, reporting, and other activities associated with the PF program. The main areas to be reviewed are the proper management and supervision, a comprehensive, well-documented formal training program, and sufficient quantities of appropriate, well-maintained, and logically deployed equipment and facilities.

The process of evaluation includes assessing the results of the survey activities (document reviews, interviews, and performance testing). Key elements of the evaluation are:

- Integration of site protection measures with the site security plans
- Analyzing data
- Developing findings, suggestions, and observations
- Recognizing noteworthy accomplishments/achievements
- Validation of observations
- Compiling field activity notes
- System performance tests.

Documentation

DOE orders require that all PF policies and procedures be properly documented. Document review will include the following documents:

- PF general and post orders
- PF shift schedules and post assignments
- PF weapons and ammunition inventories
- Vehicle maintenance records
- Weapons maintenance logs
- Response Plans
- Recapture/Recovery Plans
- Explosive Detection Plans
- Memoranda of Understanding with local law enforcement agencies and documentation of exercises conducted with those agencies
- Protective Force Training Plan
- PF training records
- A list of PF personnel who are subject to weapons qualification within 90 days of the start date of the survey
- A list of PF personnel who are medically certified to participate in the physical fitness program
- All documentation of PF exercises conducted since the last DOE Safeguards and Security Survey
- Job task analyses (JTA)

Documents will be thoroughly reviewed to:

- Ensure compliance with DOE directives
- Identify inconsistencies and contradictions
- Ensure understanding of, and familiarity with, the PF
- Develop ideas for system performance testing
- Identify deviations to DOE directives

Interviews

Meetings will be scheduled and interviews conducted with the following:

- PF management
- PF supervisors
- PF training staff
- Special Response Team (SRT) leaders
- Security police officers (SPOs) and security officers (SOs)
- Facility safeguards and security management (concerning interface with PF)
- PF safety managers

Virtually any member of the PF, from the manager to a recruit undergoing basic training, is a potential interview candidate. Facility employees who are not members of the PF may be interviewed to provide information about PF practices they observe. While interviews can be used to round out the survey team's knowledge of the PF, their more important function is to help determine the knowledge and perceptions of individuals. Members of the PF may be interviewed on or off post to determine their perception, understanding, and knowledge of policies, procedures, requirements, and duties.

The processes of evaluation include assessing the results of the above activities (document reviews, interviews, and performance testing). Key elements of the evaluation are:

- Coordination
  - PF elements (SPO, SRT, etc.)
  - PF and Local Law Enforcement Agencies
  - PF and FBI
- Integration
  - Basic training with site-specific job task
  - SRT training with tasks associated with SRT duties
- Analyzing data
- Developing findings, suggestions, observations
- Recognize noteworthy accomplishments/achievements
- Validation of observations
- Compiling field activity notes
- Implementation of written procedures
- Adequacy of protective equipment and vehicles

Performance Measures

Performance testing of a PF involves a wide range of activities from the very simple to the very complex. Performance tests are used to realistically evaluate, and verify the effectiveness of PF programs; identify and provide training for personnel; identify areas requiring system improvements; validate implemented improvements; and motivate PF personnel.

PF performance tests are divided into six types: 1) Limited Scope Performance Tests (LSPTs), 2) Alarm Response and Assessment Performance tests, 3) Force-On-Force (FOF) exercises, 4) Command Post Exercises, 5) Command Field Exercises, and 6) Joint Training Exercises. At a minimum, LSPTs will be conducted to test the following elements of the PF system and organization:

- Firearms qualification proficiency
- Physical fitness proficiency
- Response to alarms and other security situations
- Command and control capabilities
- Special Response Team (SRT) tactics and capabilities
- SPO knowledge and proficiency with issued equipment (handcuffs, OC spray, gas masks, etc.)
- SPO or SO personnel knowledge of DOE use of force criteria, approved facility general orders, post orders and procedures
- Operation and reliability of assigned equipment and vehicles

Other exercises may be performed as appropriate for the facility. All performance tests must be planned, coordinated, documented and executed as specified in the Site's Performance Testing Procedures.

Performance tests, of whatever type, generally lend themselves to being conducted on either an announced or unannounced basis. Unannounced performance tests require special planning and coordination to ensure safety and minimum disruption of facility operation. For this reason, a knowledgeable "trusted agent" should be provided by senior facility management to the survey team.

Major aspects of the coordination, planning, conduct and results of PF performance test will be documented in the survey report. A written test plan will be prepared for PF performance testing activities. The plan will consider and include, as appropriate:

- The specific element of the PF being tested;
- The objective of the test;
- Applicable pass/fail criteria;
- Specific safety considerations;
- Specific safeguards and security considerations;
- Test results documentation and after action reviews; and
- Classification of the proposed test and anticipated results, as appropriate.

PF performance tests will be conducted with the highest regard for the safety and health of personnel, protection of the environment, and protection of government property.

Annual requirements for Force-On-Force exercise, Command Post exercise, and Command Field exercise may be combined where determined appropriate in Site Safeguards and Security

Plans. Requirements for Alarm Response and Assessment Performance Tests may also be satisfied through combined testing of multiple alarms in the same or proximate location(s).

D. Security Badges, Credentials, and Shields

A security badge system or personal recognition is used at DOE and DOE contractor facilities involving security interests to provide a means for ensuring that only authorized personnel enter, occupy, or leave, and to indicate limitations placed on access.

A badge system is used to control access to facilities with security interests or security areas in which thirty (30) or more persons are employed. If a badge system is not used, the nature of the activities and involvement permit adherence to a personal recognition system which provides a high level of assurance that unauthorized persons will be denied.

There will be records pertaining to the security badge, credential, and shield accountability system and they should indicate the disposition of all badges, including date of issuance, name of holder, and type of access authorization.

Survey Content

Evaluation of the planning, implementation, and management of the Security Badges, Credentials, and Shields will include planning documents, management support/involvement, administration of the program, staffing qualifications, reporting, and other activities. The main elements to be reviewed are the handling, storage, and transmitting procedures and practices of the badging system; procedures for lost or forgotten badges; and procedures for recovering badges including procedures for retrieving badges from employees terminating under unusual circumstances.

A review should be made of the records of lost badges. Inspectors should review the procedures for notifying personnel controlling access to security areas of lost badges. The storage location of badges, inserts, and plates should be inspected to ensure they are being protected against loss, theft, or unauthorized use. The records should show that annual inventories are conducted of blank inserts and plates, and that inventory records are maintained.

Procedures for issuing temporary badges should show that records used to verify clearances are up to date. Visitor logs and records are reviewed to ensure that positive identification is made before visitors enter. Visitor badging records are to be reviewed to ensure that appropriate records are maintained and that badges are issued only for the appropriate dates.

The process of evaluation includes assessing the results of the survey activities. Key elements of the evaluation are:

- Integration of site protection measures with security plans
- Analyzing data

- Developing findings, suggestions, and observations
- Recognizing noteworthy accomplishments/achievements
- Validation of observations

Documentation

A personnel identification system should identify those personnel who are authorized to enter or leave security areas and should indicate limitations on their movement or access to classified matter. In addition, the following documentation must be reviewed:

- Access/Badge control procedures (automated and manual)
- Badge/pass information contained on the front of the badge
- Policies/procedures for issuing, recovering, and replacing badges
- Inventories of blank stock and visitor badges

Documents must ensure compliance with DOE policy and should not reflect inconsistency or contradictions.

Interviews

Interviews must be conducted with the following individuals:

- Safeguards and Security Management
- Protective Force personnel
- Badge office management
- Others responsible for access control

Performance Measures

The tamper-resistance of badge/pass documents and the effectiveness of the entry-control systems should be performance tested.

E. Transportation Security

Surveys of SNM and/or sensitive information pertaining to shipping operations are limited to survey of physical and technical protection provided in transit. Coordination with other operation groups may be necessary to ensure and adequate survey of this subtopical area. Shipment surveys should be conducted on an as-needed basis.

Survey Content

Evaluation of transportation of SNM and other sensitive information should include planning documents, management support/involvement and administration of the program, reporting, and other activities. The main elements to be reviewed are the handling, and transporting procedures and practices of SNM, sensitive matter, and DOE property.

The process of evaluation includes assessing the results of the survey activities. Key elements include:

- Site transportation practices
- Data analysis
- Findings, suggestions, and observations
- Recognizing noteworthy accomplishments
- Validation of observations

Documentation

During the survey, Inspectors must review:

- Security Plans
- Shipment procedures
- In-transit emergency plans
- Shipment emergency response plans

Documents must be thoroughly reviewed to ensure compliance with DOE policy and to identify inconsistencies and contradictions.

Interviews

Inspectors should interview:

- Shipping Program Management
- Designated Responders
- Emergency Operations Center personnel
- Warehouse personnel
- Drivers, pilots, and escorts

Performance Measures

Shipment surveys do not lend themselves to performance testing. The most effective way to survey this element is to accompany a randomly selected shipment. The shipment should be observed from loading to unloading. This allows the inspectors to determine if the appropriate procedures are being followed; that adequate surveillance is maintained; and appropriate emergency procedures are followed.